

DID YOU KNOW?

The pound recently fell to a 31-year low. Whilst at first glance this may appear to be a cause for concern, the pound's reduced value has provided a boost to the nation's productivity. In fact, according to the Office for National Statistics, output per hour has increased by 0.6 per cent, which has helped Britain to recover from the last vestiges of the 2008 downturn. This reinvigorated economic climate has also helped the nation's business confidence bounce back to pre-Brexit levels.



IN THIS ISSUE

Internet of Things Promises Huge Rewards, But It Is Not Risk-free

The Internet of Things is poised to revolutionise how we conduct business, yet many companies are ill-prepared to properly incorporate the technology into their day-to-day operations.

SMEs Missing Out on Billions in Export Sales

Less than a fifth of SMEs are taking advantage of the international opportunities that Brexit has provided.

Companies Double Cyber Security Spend yet Still Lack Basic Knowledge

Whilst companies are spending more than ever on cyber security, they still lack an understanding of how their digital defences work.

Internet of Things Promises Huge Rewards, But It Is Not Risk-free

A new study from 25 data protection regulators from around the world, including the Information Commissioner's Office, found severe pitfalls for any business hoping to take advantage of the Internet of Things (IoT). The IoT is a vast interconnected system of devices, vehicles and even entire buildings capable of connecting to the internet and communicating with each other. And it promises big benefits. In fact, about 25 per cent of global manufacturers are already using IoT technology to streamline their operations, according to the government. Businesses in all industries can use the IoT to monitor water usage and overall energy use; thus, saving money and minimising consumption—not to mention the industry-specific benefits. For example, using IoT technology in the retail sector to improve inventory management could save UK retailers £3 billion over the next several years, according to a Morgan Stanley report. And research from the Centre for Economics and Business Research estimates that the IoT and big data analytics will add £322 billion to the economy from 2015 to 2020.

Yet, despite the potential benefits of using the IoT, the report found severe pitfalls—primarily with how it collects, stores and distributes your data. According to the report, 3 out of 5 IoT devices do not properly tell customers how their personal information is being used. What's more, nearly 3 out of 4 devices failed to adequately explain how users can delete their information. These glaring omissions could leave companies vulnerable to cyber attacks. In fact, less than 1 out of 3 companies are prepared to handle the cyber security risks associated with the IoT, according to a survey conducted by Tripwire, a software company.

If your company chooses to integrate IoT devices into your regular business operations, consider using these best practices:

- Provide your employees with comprehensive training on how to use each IoT device—including how to delete any unnecessary or sensitive information.
- Inspect your cyber security system to confirm that each device has adequate cyber protections.
- Schedule regular maintenance for your IoT devices to ensure that their software is up to date and they have the latest patches.



**Crendon
Insurance
Brokers**

SMEs Missing Out on Billions in Export Sales

Despite the growing demand for British-made goods, less than 20 per cent of UK SMEs currently sell their goods to customers abroad, according to a recent report from the Centre for Economics and Business Research. An explanation for this limited participation could stem from the difficulties encountered by SMEs in their efforts to expand into new international markets. These barriers to trade often include international shipping costs, concerns about foreign customs and duties, and insurance costs.

Yet, if the number of SMEs that are able to successfully overcome these trade barriers increases to just 40 per cent, that effort would contribute an estimated £141.3 billion to the economy. Whilst it may seem like a daunting challenge to double the number of SMEs conducting business with overseas customers, business owners are optimistic that they will be able to meet that mark. In fact, nearly 48 per cent of SMEs believe that they will experience growth in international trade in the near future, according to a survey conducted by market research firm East and Partners. This confidence can be directly attributed to a weaker pound and a renewed sense of freedom from the EU's red tape—both of which are repercussions of Brexit.

Possibly the most straightforward strategy for SMEs to adopt in order to reach international clients would be to set up a robust online store and contact a Department for International Trade adviser for a free consultation by visiting www.greatbusiness.gov.uk/ukti. To make your business' website more accessible, consider making these five changes:

1. Offer customers the option of paying with multiple types of currency.
2. Provide customers with the ability to change the language on your website.
3. Keep your shipping costs low.
4. Build and maintain an online presence on several different social media platforms, such as Instagram, Twitter and Facebook.
5. Invest in search engine optimisation to ensure potential international customers can find your online store quickly and easily.

CI PROFILE

Companies Double Cyber Security Spend yet Still Lack Basic Knowledge

If your company were to experience a cyber security incident—such as a security breach or cyber attack—you should expect to pay an average of £2.6 million, which is more than double the cost in 2015, according to a new report from PricewaterhouseCoopers (PwC). What's more, the impact of these incidents can be so significant that nearly 4 out of 5 companies experience downtime as a result. During these periods of business disruptions, you may experience further knock-on effects such as extra expenses, supply chain disruptions and reputation damage.

To combat this threat, companies are spending an average of £6.2 million on cyber security, which is double what they spent in 2015. Yet, whilst companies are spending more on cyber security, many are foregoing the additional cost of cyber cover, which leaves them dangerously exposed. Only 38 per cent of companies are insured against cyber threats, according to PwC.

To ensure that cyber defences are effective, companies need robust cyber cover as well as a holistic understanding of how cyber security works and what the common risks are—which a significant number of companies still lack. Merely 28 per cent of companies have board members that contribute to the development of a cyber security strategy, whilst only 33 per cent have board members that are directly involved in setting up their cyber security budgets. This minimal participation can inadvertently create potential gaps in a company's cyber security that criminals could exploit.

To ensure that your company's cyber security system is comprehensive and effective, you should provide annual cyber security training for your entire staff—from interns all the way up to directors and officers. This training should include how to identify common cyber threats, password best practices and the procedure for a cyber security breach. And of course, all businesses need comprehensive cyber cover.

If your company is interested in additional guidance on how to develop an effective cyber security system, the National Cyber Security Centre has released a [10-step guide](#). For other cyber security enquiries, contact the insurance professionals at **Crendon Insurance Brokers Ltd** today.

The Rising Costs of Cyber Breaches

